UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/708,197	02/16/2004	Arkady Berenstein		2196

34069 7590 02/06/2007

LEON CHERNYAK
112 ACADEMY HILL RD. #1
BRIGHTON, MA 02135

EXAMINER	
GELAGAY, SHEWAYE	
ART UNIT	PAPER NUMBER
2137	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/708,197	BERENSTEIN ET AL.	
	Examiner	Art Unit	
	Shewaye Gelagay	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3 and 10-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *1-3 and 10-22* is/are rejected.

7)☐ Claim(s) *4-9,12,13 and 23-41* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *2/16/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Oath/Declaration

1. The oath or declaration is defective. A new oath or declaration in compliance with 37 CFR 1.67(a) identifying this application by application number and filing date is required. See MPEP §§ 602.01 and 602.02.

The oath or declaration is defective because: It is not signed by the inventors.

Claim Objections

2. Claims 4-9, 12-13, 23-41 are objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent claim should refer to other claims in the alternative only. See MPEP § 608.01(n). Accordingly, the claims have not been further treated on the merits.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 16, 20 and 22 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed,

had possession of the claimed invention. Claims 16, 20 and 22 recite "Hermitian vector space", however, the "Hermitian vector space" is not disclosed in the specification. The specification as filed does not mention the use of "Hermitian vector space".

5. Claim 18 depend from claim 16, hence inherit the deficiencies of claim 16.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-3, 10-11, 14-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Anshel et al. (hereinafter Anshel) US Patent Number 6,493,449 in view of Hoffstein et al. (hereinafter Hoffstein) US Patent Number 6,298,137.

As per claim 1:

Anshel teaches a method of secure distribution of encryption/decryption keys among two communicating parties by providing secure algebraic key establishment protocols. Users A and B wish to exchange keys via public discussion over insecure channel, user A randomly chooses elements S1, ..., Sn element of G and transmits them to user B via the communication module. Similarly user B randomly chooses elements t1,...,tm and transmits them to user A via the communication module, wherein s1,...,sn and t1,...,tn are publicly known. And generate a word a which is a secret word in the generators s1,...sn, and generate a word b which is a secret word in the

generators t1, ...,tn. The secret word a together with the generators t1,...,tn and the secret word b with generators s1,...,sn are presented to compute conjugate elements. (col. 9-col.13)

Anshel does not expressly disclose computing the n-tuple g^A by the first communicating party and transmitting it to the second communicating party and generating g^B by the second communicating party and transmitting it to the firs communicating party. However, Hoffstein teaches computing the n-tuple g^A by the first communicating party and transmitting it to the second communicating party and generating g^B by the second communicating party and transmitting it to the firs communicating party. (Abstract; col. 11, line 63-col. 13, line 30) Therefore it would have been obvious to one ordinary skill in the art to modify the method disclosed by Anshel with Hoffstein in order to have a system that combines relatively short, easily created keys, with relatively high speed encoding and decoding process. (col. 2, lines 30-33; Hoffstein)

As per claims 2 and 10:

The combination of Anshel and Hoffstein teaches all the subject matter as discussed above. In addition, Anshel further discloses a method wherein G is an arbitrary compact topological monoid and the polynomials p(x.sub.1, x.sub.2, . . . x.sub.k) and q(x.sub.1, x.sub.2, . . . , x.sub.k) have non-negative integer coefficients, and all the matrices S.sub.1, S.sub.2, . . . , S.sub.k have non-negative integer matrix coefficients. (col. 9-col.13)

As per claims 3 and 11:

The combination of Anshel and Hoffstein teaches all the subject matter as discussed above. In addition, Anshel further discloses a method wherein G is an arbitrary compact topological group and the polynomials p(x.sub.1, x.sub.2, . . . x.sub.k) and q(x.sub.1, x.sub.2, . . . , x.sub.k) have arbitrary integer coefficients, and all the matrices S.sub.1, S.sub.2, . . . S.sub.k have arbitrary integer matrix coefficients. (col. 9-col.13)

As per claims 14-22:

The combination of Anshel and Hoffstein teaches all the subject matter as discussed above. In addition, Hoffstein further discloses a method wherein n=1 and said G is a connected closed subgroup of the orthogonal group O(V), where V is a Euclidean vector space. (col. 6, lines 63-67)

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See Form PTO-892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shewaye Gelagay

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER